Images of word maps in almost simple groups and quasisimple groups

MATTHEW LEVY

Imperial College London

Abstract

It has been shown by Lubotzky in [10] that the set of verbal images of a fixed non-abelian finite simple group G is precisely the set of endomorphism invariant subsets of G. Here we use his result to determine the verbal images of certain almost simple groups and quasisimple groups.

1 Introduction

Let w be a word in the free group of rank k. For any group G we can define a word map $w : G^k \to G$ and we shall let $w(G)$ denote the set of word values, i.e. $w(G) := \{w(g_1, ..., g_k) : g_i \in G\}$, we will call this the *verbal image* of w over G. There has recently been much interest and progress in the study of verbal images over finite groups though the topic has grown from work first begun by P. Hall, see [13] for a modern exposition.

In [7] it is shown that for any alternating group $\mathrm{Alt}(n)$ with $n \geq 5$ and $n \neq 6$ there exists a word w such that $\mathrm{Alt}(n)_w$ consists of the identity and all 3-cycles. This result also holds for $\mathrm{Sym}(n)$. They also construct words whose image over $\mathrm{Alt}(n)$ is the identity and all p-cycles for any prime $3 < p < n$ and $n \geq 5$. All these words are explicitly given and they go on to give other explicit examples of words whose verbal image over a given group is a single automorphism class and the identity. Other examples can also be found in [8].

In [10] Lubotzky has proved that any automorphism invariant subset that contains the identity of any non-ableian finite simple group can be obtained as the image of a word map in two variables. His proof requires the classification of finite simple groups (CFSG). In particular, it uses a result by Guralnick and Kantor [4] which asserts that any non-identity element of a finite simple group is part of a generating pair. In this article we will extend some of the arguments used by Lubotzky to make similar statements for certain almost simple groups and quasisimple groups thus some of our results also depend on the classification. Our main results are:

Theorem A. *The verbal images of S_n are either:*

i) an $\mathrm{Aut}(S_n)$-invariant subset of A_n including the identity or;

ii) the union of an $\mathrm{Aut}(S_n)$-invariant subset of S_n and C, where C is the set of all 2-power elements of S_n.

Theorem B. *There exists a constant C with the following property: Let S be a universal quasisimple group with $|S| > C$ and let A be a subset of S such that $e \in A$ and A is closed under the action of the automorphism group of S. Then there exists a word $w \in F_2$ such that $w(S) = A$.*

2 Almost simple groups

Let G be an almost simple G, i.e. we have $S \leq G \leq \mathrm{Aut}(S)$ where S is the unique minimal normal non-abelian simple characteristic subgroup of G. A well-known corollary of the CFSG is that $\mathrm{Aut}(S)/S$ is solvable hence so is G/S. The group G also has the property that any subgroup not containing S doesn't contain S as a composition factor, that is if $H \leq G$ with $S \not\leq H$ then $S \notin \mathrm{Comp}(H)$, where $\mathrm{Comp}(H)$ is the set of composition factors of H. To see this observe that if $H \leq G$ with $S \in \mathrm{Comp}(H)$ then since $H/H \cap S$ is

solvable we must have that $S \in \text{Comp}(H \cap S)$ thus $S = H \cap S$ giving $S \leq H$. Now suppose that $G \trianglelefteq \text{Aut}(S)$ then we have $\text{Aut}(K) \leq \text{Aut}(G) = \text{Aut}(S)$ for any $S \leq K \leq G$. For the remainder of this section we fix an almost simple group G with $S \leq G \trianglelefteq \text{Aut}(S)$ where S is a non-abelian finite simple group. We will combine arguments of Abért in [1] and Lubotzky in [10] to prove the following theorem:

Theorem 2.1. *Let A be a subset of S such that $e \in A$ and A is closed under the action of the automorphism group of G where G and S are as above. Then there exists a word $w \in F_2$ such that $w(G) = A$.*

Lubotzky's proof involves studying subdirect products of simple groups. We would like to generalise some of his argument to work for almost simple groups. This is where we use a result of Abért where he studied such subdirect products, more specifically he looked at subdirect products of just non-solvable groups. The following lemma is due to Abért ([1]) but has been adapted:

Lemma 2.2. *Consider $P = G_1 \times ... \times G_n$ where each $G_i \cong G$. Denote by S_j the minimal normal subgroup of G_j so that each S_j is isomorphic to S. Now let $a_{i,j} \in G_j$ for $1 \leq i \leq k$ and $1 \leq j \leq n$, and suppose that*

$$< a_{1,j}, ..., a_{k,j} > = G_j \text{ for } 1 \leq j \leq s;$$
$$< a_{1,j}, ..., a_{k,j} > = B_j \geq S_j \text{ for } s < j \leq n,$$

and that for $1 \leq j < l \leq n$ the k-tuples $(a_{1,j}, ..., a_{k,j})$ and $(a_{1,l}, ..., a_{k,l})$ are automorphism independent over G. For $1 \leq i \leq k$ let

$$h_i = (a_{i,1}, ..., a_{i,n}) \in G_1 \times ... \times G_n$$

and let

$$H = < h_1, ..., h_k > \leq G_1 \times ... \times G_n.$$

Then

$$M = S_1 \times ... \times S_n \leq H.$$

Before proceeding with the proof of the lemma we first note that, setting $n = s + t$, the above lemma holds in the case where $t = 0$; this is proved in [1]. We also recall the following from [1] though it is not stated in this way:

Lemma 2.3. *Let $H \leq P$ be a subgroup containing M such that*

$$\pi_j(H) = G_j \text{ for } 1 \leq j \leq s;$$
$$\pi_j(H) \geq S_j \text{ for } s < j \leq n,$$

where π_j denotes the projection to the j-th component. Let K be a normal subgroup of H. Then

$$K \cap M = \prod_{\pi(K) \neq 1} S_j.$$

Proof. Since $K \cap M$ is normal in $M = \prod_{1 \leq j \leq n} S_j$ it is the direct product of some of the S_j, say

$$K \cap M = K_1 \times ... \times K_n,$$

where $K_i = S_i$ or 1.
   If $\pi_j(K) = 1$ then $K \cap S_j = 1$ so $K_j = 1$.
   If $\pi_j(K) \neq 1$ then $\pi_j(K) \trianglelefteq \pi_j(H)$ so $S_j \leq \pi_j(K)$ by minimality of S_j. Thus

$$K \cap M \geq [K, M] \geq [K, S_j] = [\pi_j(K), S_j] = S_j,$$

so $K_j = S_j$. $\qquad\square$

Proof of Lemma 2.2. Consider the projection to the first $n - 1$ coordinates:

$$f : G_1 \times ... \times G_s \times B_{s+1} \times ... \times B_n \to G_1 \times ... \times G_s \times B_{s+1} \times ... \times B_{n-1}.$$

Let $H_1 = f(H)$ and let $R = \pi_n(\text{Ker}(f)) \trianglelefteq B_n$. By induction on n and the above remark, we have $S_1 \times ... \times S_{n-1} \leq H_1$ and by minimality of S either $R \geq S_n$ or $R = 1$.

We claim that $S_n \leq R$. Assume, for contradiction, that $R = 1$. Define the map $\theta : H_1 \to B_n$ by

$$\theta(g_1, ..., g_{n-1}) = g_n \text{ if } (g_1, ..., g_{n-1}, g_n) \in H.$$

Since $(g_1, ..., g_{n-1}, g_n), (g_1, ..., g_{n-1}, g'_n) \in H$ implies $g_n^{-1} g'_n \in R$, θ is a well-defined, surjective homomorphism. We are also using the fact that $< a_{1,n}, ..., a_{k,n} > = B_n$. Now let $K = \text{Ker}(\theta) \trianglelefteq H_1$ and so

$$H_1/K \cong B_n \trianglerighteq S_n,$$

which is not solvable and has S as a composition factor. Since $S_1 \times ... \times S_{n-1} \leq H_1$, by lemma 2.3

$$K \cap M = \prod_{\pi(K) \neq 1} S_j.$$

If $K \geq M$ then H_1/K would be solvable, a contradiction. So there exists a coordinate $1 \leq l < n$ such that $\pi_l(K) = 1$, i.e. $K \leq \text{Ker}(\pi_l)$. Since

$$H_1/\text{Ker}(\pi_l) \cong B_l \trianglerighteq S_l$$

is a quotient of H_1/K with S as a composition factor we must have $K = \text{Ker}(\pi_l)$. This means that the function $\alpha : B_l \to B_n$ given by

$$\alpha(g_l) = g_n \text{ if } (g_1, ..., g_l, ..., g_n) \in H$$

is an isomorphism, i.e. $B_l \cong B_n \cong B$, say. Thus $\alpha(a_{i,l}) = a_{i,n}$ for $(1 \leq i \leq k)$ which in turn implies that the tuples $(a_{1,l}, ..., a_{k,l})$ and $(a_{1,n}, ..., a_{k,n})$ are not automorphism independent over B and hence G, a contradiction. Hence the claim holds and $1 \times ... \times 1 \times S_n \leq H$.

Now let $L = f^{-1}(S_1 \times ... \times S_{n-1}) \leq H$ and denote by $L^{(i)}$ the i-th term of the derived series of L and let r be a number such that $L^{(r)} = L^{(r+1)}$. Then $f(L^{(r)}) = S_1 \times ... \times S_{n-1}$ and since $1 \times ... \times 1 \times S_n \leq L$ it follows that $1 \times ... \times 1 \times S_n \leq L^{(r)}$. But $J = \pi_n(L^{(r)}) \trianglelefteq B_n$ and $J = J'$ and so $J = S_n$. Finally, this implies that

$$L^{(r)} = S_1 \times ... \times S_n \leq H.$$

$\square$

We will now follow Lubotzky's argument making use of the above lemma along the way.

2.1 Proof of 2.1

Let $\Omega = \{(a_i, b_i) : i = 1, ..., |G|^2\}$ be the set of all ordered pairs of elements from G such that the first l pairs generate a subgroup of G containing S and the remaining pairs generate proper subgroups of G not containing S and thus don't contain S as a composition factor. Consider the homomorphism from $F_2 = < x, y >$, the free group on two letters, to the direct product of $|\Omega|$ copies of G, $\phi : F_2 \to \prod_\Omega G$ where $\phi = \prod_\Omega \phi_i$ and each ϕ_i is given by the unique homomorphism from F_2 to G sending x to a_i and y to b_i. Write Ω as the disjoint union of Ω_1 and Ω_2 where Ω_1 is the set of the first l 'generating' pairs in Ω and Ω_2 is the set of the remaining 'non-generating' pairs and write $G_i = \prod_{\Omega_i} G$ accordingly. Set $r_1 = (a_1, ... a_l)$ and $r_2 = (b_1, ..., b_l)$ and consider the subgroup of G_1 generated by r_1 and r_2, $R = < r_1, r_2 >$. Then by lemma 2.2, R contains a subgroup E_1 isomorphic to S^r for some r depending on the number of automorphism independent orbits of Ω_1. It turns out that $r = \frac{l}{|\text{Aut}(G)|}$:

To see this note that an element $c = (c_1, ..., c_l)$ is in E_1 if and only if whenever $\alpha \circ \phi_i = \phi_j$ for some $1 \leq i, j \leq l$ and $\alpha \in \text{Aut}(G)$, $\alpha(c_i) = c_j$. Now, the group $\text{Aut}(G)$ acts freely on the pairs in Ω_1 and similarly on the set of homomorphims $\{\phi_i : i := 1, ..., l\}$. Indeed, if $\alpha \in \text{Aut}(G)$ and $\alpha \circ \phi_i = \phi_j$ (or equivalently, $(\alpha(a_i), \alpha(b_i)) = (a_i, b_i)$) then α is the identity automorphism of G. It follows that the l epimorphisms form $r = l/|\text{Aut}(G)|$ orbits.

Fix r representatives for the orbits of Ω_1 and denote this set by Ω_r. Now we have to worry about the remaining 'non-generating' pairs. Set $h_1 = (a_i)$ and $h_2 = (b_i)$ and let $H = < h_1, h_2 >$. Consider the subgroup D of H whose projection to G_1 is E_1. We claim that this subgroup is of the form $E_1 \times E_2$ where E_2 is its projection to G_2. Let K_i denote the kernel of the projection from D to G_i for each i so that $D/K_i \cong E_i$. Now K_1 is a subgroup of E_2 whose projection to every single copy of G in E_2 is a proper subgroup of G hence K_1 has no composition factor isomorphic to S. Since $E_1 \cong D/K_1$ is isomorphic to S^r we must have that $E_1 = K_2$. This is because K_2 is a subgroup of E_1 and both are isomorphic to S^r as every one of

the r composition factors isomorphic to S should appear in K_2 as $E_2 \cong D/K_2$ has no composition factor isomorphic to S. Thus $D = E_1 \times E_2$ where E_1 is a diagonally, twisted by automorphisms, embedded subgroup of G_1 isomorphic to S^r. We have proved the following:

Proposition 2.4. *With the notation as above we have*

$$H \geq D = E_1 \times E_2 = \prod_{(a,b)\in\Omega_r} D(S,(a,b)) \times E_2 \leq \prod_\Omega G.$$

Here $D(S,(a,b))$ is a diagonal subgroup of $\prod_{\Omega^{Aut(G)}_{(a,b)}} G$ isomorphic to S where $\Omega^{Aut(G)}_{(a,b)}$ is the orbit of the pair $(a,b) \in \Omega$ under $Aut(G)$. More specifically, $D(S,(a,b)) = \{(g^\phi)_{\phi\in Aut(G)} : g \in S\}$.

We continue with Lubotzky's proof: A result of Guralnick and Kantor (see [4]) says that for every non-abelian finite simple group S and for every $e \neq a \in S$ there exists $b \in S$ such that a and b generate S. Now suppose the set $A' = A \setminus \{e\} < S$ is a union of k $Aut(G)$-orbits and let $T = \{z_1, ..., z_k\}$ be a set of representatives for these orbits. It follows that for every $z \in T$ there exists an $1 \leq i \leq l$ such that $z = a_i$ with $(a_i, b_i) \in \Omega_1$ and observe that the orbit of z under $Aut(G)$ gives an orbit of (a_i, b_i). It is clear that $k \leq r$.

Define the following element $v = (v_i) \in G_1 \times G_2$ by

$$v_i = \begin{cases} a_i & \text{if } a_i \in A' \text{ and } 1 \leq i \leq l; \\ e & \text{otherwise.} \end{cases}$$

It is easy to see that the above element v is an element of H. Indeed its projection to G_2 is the identity and its projection to G_1 lies in E_1 by definition and the fact that A is $Aut(G)$-invariant. We also observe that the Guralnick-Kantor result ensures that every element of A appears as a coordinate entry of v. This means that there exists an element $w \in F_2$ such that its image in $H = \phi(F_2)$ is $\phi(w) = \prod_\Omega \phi_i(w) = (w(a_i, b_i)) = v$. This word w has the required property, i.e. $w(G) = A$.

2.2 Verbal images of Symmetric Groups

As remarked by Lubotzky in [10] his proof actually shows, for example, the existence of a word with the following property:

$$w(a,b) = \begin{cases} v(a,b) & \text{if } <a,b> = G; \\ e & \text{otherwise,} \end{cases}$$

where v is any fixed word and G a simple group. In fact, we could choose a different word v for each distinct $Aut(G)$-orbit of the set of pairs of generators. We will make use of this remark as well as the above theorem to classify the verbal images of S_n.

For now we will fix $n \geq 5$. As remarked by Kassabov and Nikolov in [7] if the image of a word w over S_n contains an element outside of A_n then it contains all elements of 2-power order. To see this note that to contain an element outside A_n the word must have a free variable with odd exponent sum, i.e. the verbal image of w contains the verbal image of x^{2m+1} for some integer m. Let C denote the set of all elements of 2-power order in S_n including the identity and let A be an $Aut(S_n)$-invariant subset of S_n. If $A \subseteq A_n$ then the above theorem shows that there exists a word with image precisely A. Suppose that A contains an element outside of A_n. It follows that A must contain C. We claim that any such A can be the image of a word map. Choose a word $v(x_1, x_2) \in F_2$ with the following property:

$$v(a,b) = \begin{cases} a & \text{if } a \in A_n, \ (o(a),2) = 1 \text{ and } a \in A; \\ a^{-e/e_2}a & \text{if } a \in A_n, \ (o(a),2) \neq 1 \text{ and } a \in A; \\ a^{o(a)_2} & \text{if } a \in S_n \setminus A_n \text{ and } a \in A; \\ 1 & \text{otherwise,} \end{cases}$$

where e is the exponent of S_n, n_2 is the 2-part of an integer n and $o(g)$ is the order of $g \in S_n$. We are also writing 1 for the identity of S_n. Such a word exists by theorem 2.1 and noting that any $a \in S_n \setminus (A_n \cup C)$ can generate S_n or A_n since by the Guralnick and Kantor result there exists a b such that $<a^2, b> = A_n$ and

so $< a,b >= S_n$ or A_n. Also recall that $\mathrm{Aut}(A_n)=\mathrm{Aut}(S_n)$ and note that for any $a \in S_n$, $a^{o(a)_2} \in A_n$. Define $w(x_1,x_2) = x_1^{e/e_2}v$ where v is as above. Then the image of w is precisely A since:

$$w(a,b) = \begin{cases} a & \text{if } a \in A_n, \ (o(a),2)=1 \text{ and } a \in A; \\ a & \text{if } a \in A_n, \ (o(a),2) \neq 1 \text{ and } a \in A; \\ a' & \text{if } a \in S_n \setminus A_n \text{ and } a \in A; \\ \in C & \text{if } a \notin A. \end{cases}$$

where $a' = a^{e/e_2+o(a)_2}$ is S_n-conjugate to a as $(e/e_2+o(a)_2, o(a))=1$.

This completes the proof of Theorem A.

3 Quasisimple groups

Recall the result of Guralnick and Kantor that says for every finite simple group $\bar{S}$ and for every $e \neq a \in \bar{S}$ there exists $b \in \bar{S}$ such that a and b generate $\bar{S}$. Now for a quasisimple group S we have that for every non-central element $a \in S$ there exists $b \in S$ such that a and b generate S. This follows from the easy fact that if a set of elements generate a perfect group modulo its centre then they in fact generate the group, i.e. if $M \leq S$ and $M Z(S) = S$ then $M = S$. We will now fix a quasisimple group S that is universal for a simple group $\bar{S}$, i.e. $\bar{S} = S/Z(S)$ and S is the unique largest such central extension of $\bar{S}$. The existence of such a S follows from facts about the Schur multiplier of $\bar{S}$ and S is also known as the Schur covering group of $\bar{S}$. In this case $\mathrm{Aut}(\bar{S})$ is equal to the group of automorphisms of $\bar{S}$ induced from $\mathrm{Aut}(S)$. In particular, this means that the action of $\mathrm{Aut}(\bar{S})$ on $\bar{S}$ is equivalent to the action of $\mathrm{Aut}(S)$ on $\bar{S}$. In this section we will use Lubotzky's result to prove the following theorem:

Theorem 3.1. *Let S be a universal quasisimple group and let A be a subset of S such that $e \in A$ and A is closed under the action of the automorphism group of S. If S has property $(*)$ then there exists a word $w \in F_2$ such that $w(S) = A$.*

The details of property $(*)$ will be given later.

3.1 Proof of 3.1

Let S be the universal Schur covering group of a finite simple group $\bar{S}$ so that $\bar{S} = S/Z(S)$. Let $\Omega = \{(a_i,b_i) : i = 1,...,|S|^2\}$ be the set of all ordered pairs of elements from S such that the first l pairs generate S whilst the remaining pairs generate proper subgroups of S. Suppose that there are r automorphism independent generating pairs modulo the centre, fixing r representatives for these we may assume that these are the first r pairs of Ω, denote this set by Ω_r. Now consider the homomorphism $\phi : F_2 \to \prod_\Omega S$ where, as before, $\phi = \prod_\Omega \phi_i$ and each ϕ_i is the unique homomorphism sending x to a_i and y to b_i with $F_2 =< x,y >$.

Write Ω as the disjoint union of Ω_1 and Ω_2 where Ω_1 is the set of the first l pairs from Ω and Ω_2 are the remaining pairs. Set $S_i = \prod_{\Omega_i} S$, $G = \prod_\Omega S$, $Z = \prod_\Omega Z(S)$ and for a subgroup K of G we will denote by $\bar{K}$ the quotient group KZ/Z. For $\Lambda \leq \Omega$ denote by S_Λ the subgroup of G whose projection to the αth component of G is S if $\alpha \in \Lambda$ and is the identity elsewhere so that $S_\Lambda \cong S^{|\Lambda|}$. When $\Lambda = \{\alpha\}$ we will just write S_α for S_Λ. Let $H =< h_1, h_2 >\leq G$ where $h_1 = (a_i)$ and $h_2 = (b_i)$. Then $\bar{H} \leq G/Z = \prod_{\bar{\Omega}} \bar{S}$. Writing $\bar{\Omega}_r$ for the set $\{(\bar{a}_i, \bar{b}_i) : i = 1,...,r\}$, the image of Ω_r modulo the centre, it follows from Lubotzky [10] that $\bar{H}$ contains a subgroup $\bar{D}$ where

$$\bar{D} = \prod_{(\bar{a},\bar{b}) \in \bar{\Omega}_r} D(\bar{S}, (\bar{a},\bar{b})),$$

where $D(\bar{(S)}, (\bar{a}, \bar{b}))$ is as in proposition 2.4.

We claim that H contains a subgroup D isomorphic to S_{Ω_r}. It is enough to prove the following: if $(a,b) = \alpha \in \Omega_r$ and $\bar{H}$ contains $\bar{S}_\alpha$ then H contains a diagonally embedded subgroup isomorphic to S_α whose projection to the α-th component of $\prod_\Omega S$ is S_α. Let $1 \neq \bar{x}, \bar{y} \in \bar{S}_\alpha$ such that $x, y \in S_\alpha$ and H contains the vectors (a_β) and (b_β) where $a_\beta \in Z(S)$ if $\beta \notin (aZ(S), bZ(S))$ and $a_\beta \in xZ(S)$ if $\beta \in (aZ(S), bZ(S))$. Similarly $b_\beta \in Z(S)$ if $\beta \notin (aZ(S), bZ(S))$ and $b_\beta \in yZ(S)$ if $\beta \in (aZ(S), bZ(S))$. Then H contains their commutator $[(a_\beta), (b_\beta)] = (c_\beta)$ where $c_\beta = e$ if $\beta \neq \alpha$ and $c_\beta = [x,y]$ if $\beta \in (aZ(S), bZ(S))$. Since S is perfect the claim follows. In summary, we have proved the following:

Proposition 3.2. *With the notation as above we have*

$$H \geq D = \prod_{(a,b)\in\Omega_r} Q(S,(a,b)) \leq \prod_\Omega S,$$

where $Q(S,(a,b))$ is a diagonal subgroup of $\prod_{(c,d)\in\Omega_{(a,b)}^{Aut(S)}} \prod_{\Omega_{(c,d)}^{Z(S)}} S$ isomorphic to S. Here $\Omega_{(a,b)}^{Aut(S)}$ is the orbit of the pair $(a,b) \in \Omega$ under Aut(S) and $\Omega_{(c,d)}^{Z(S)} = \{(cz_1,dz_2) : z_i \in Z(S)\} \leq \Omega$. More specifically, $Q(S,(a,b)) = \{(g^\phi,...,g^\phi)_{\phi\in Aut(S)} \in \prod_{\phi\in Aut(S)} \prod_{\Omega_{(a^\phi,b^\phi)}^{Z(S)}} S : g \in S\}$.

Suppose that A is an Aut(S)-invariant subset and $A' = A \setminus \{e\}$ has representatives $\{a_1,...,a_k\}$ where $k = k(A)$. Let $\{(x_i,y_i) : i = 1,..,r\}$ be representatives for Aut(S)-independent generating pairs for S that are simultaneously distinct modulo the centre of S. Since $\phi(F_2)$ contains a subgroup isomorphic to S^r we require that $r \geq k$. We will then be able to show the existence of a word with the desired property by using the usual argument; define a word $w \in F_2$ such that $w(x_i,y_i) = a_i$ for $i = 1,...,k$ and takes the identity elsewhere. We are ready to define property $(*)$:

Property $(*)$: With the notation as above, we say that a group S has property $(*)$ if $r \geq k$ for all A.

Note that a group S has property $(*)$ if and only if the above inequality holds for $A = S$. In the next few sections we will use various results about the probability that a random pair of elements generate a group and bounds on number of conjugacy classes in order to give examples of groups with property $(*)$. It is worth pointing out at this stage that the above argument already shows that if A consists of the identity and a single automorphism class then A is the image of a word map.

3.2 Covers of Alternating Groups

In this section we continue the above discussion but will focus on the subcase where $\bar{S}$ is an alternating group of degree $n \geq 5$ and S is its Schur covering group. Then for $n \neq 6,7$ we have $S = 2.\mathrm{A}_n$, the double cover of A_n, and for $n = 6$ or 7 we have $S = 6.\mathrm{A}_n$. By [11] the number of conjugacy classes, $k(G)$, of a subgroup of S_n with $n \geq 3$ satisfies $k(G) \leq 3^{(n-1)/2}$. It follows that $k(S) \leq 6.3^{(n-1)/2}$. On the other hand by [12] the probability, $p(\mathrm{A}_n)$, that a random pair of elements generate A_n with $n \geq 4$ satisfies $1 - 1/n - 13/n^2 < p(\mathrm{A}_n) \leq 1 - 1/n + 2/3n^2$. Hence the number of automorphism independent generating pairs in S $d(S) \geq d(\bar{S}) \geq p(\bar{S})|\bar{S}|^2/|\mathrm{Aut}(\bar{S})| = p(\bar{S})|\bar{S}|/|\mathrm{Out}(\bar{S})|$. For $n = 5$ we see that $d(2.\mathrm{A}_5) \geq 9$ whilst $k(2.\mathrm{A}_5) = k(\mathrm{SL}(2,5)) = 9$. For $n = 6$, as $k(\mathrm{A}_6) = 7$, a simple calculation shows that $k(6.\mathrm{A}_6) \leq 6.7 \leq (17/36).(6!/8) \leq d(6.\mathrm{A}_6)$. By induction, one can show that for $n \geq 7$, $k(S) \leq d(S)$ holds.

3.3 Groups of Lie type

Here we consider the case when S is a group of Lie type. As in the case with covers of alternating groups we need good bounds on the number of conjugacy classes and the probability that a random pair of elements generates the group. We will first deal with special linear groups and then look at the general case. For more details about groups of Lie type see, for example, [5] or [2].

3.3.1 Special Linear Groups

S will denote $\mathrm{SL}(n,q)$ a special linear group of degree n over a finite field of size $q = p^r$ of characteristic p and so $\bar{S} = \mathrm{PSL}(n,q)$. From [4] we have that the probability that a random pair of elements of $\bar{S}$ generate the group $p(\bar{S}) \geq 1 - cn^3(\log_2 q)^2/q^{n-1}$ where $c = 36$ for $n \geq 10$ and $c = 10^{10}$ if $n \leq 9$. It follows that the number of automorphism independent generating pairs $d(S) \geq d(\bar{S}) \geq p(\bar{S})|\bar{S}|^2/|\mathrm{Aut}(\bar{S})| = p(\bar{S})|\bar{S}|/|\mathrm{Out}(\bar{S})|$. Now $|\mathrm{Out}(\bar{S})| \leq 2(n,q-1)\log_p q$ and $|\bar{S}| = q^{\binom{n}{2}} \prod_{i=2}^n (q^i-1)/(n,q-1)$. Putting all this together we have

$$d(S) \geq \frac{(q^{n-1} - cn^3(\log_2 q)^2)q^{\binom{n}{2}} \prod_{i=2}^n (q^i-1)}{2q^{n-1}(n,q-1)^2 \log_p q}.$$

On the other hand a result of Fulman and Guralnick, see [3], says that the number of conjugacy classes $k(S) \leq q^{n-1} + 3q^{n-2}$. Suppose $n \geq 10$ then we have $d(S) \geq k(S)$ for all $q \geq 4$, for $n \leq 9$ we require that $q \geq 10^{15}$.

In the case where $n = 2$ and $q = p$, a prime, we can make the following estimates (see [6]):

$$p(S) \geq 1 - 1/p - 10/p^2;$$
$$k(S) \leq p + 4.$$

Putting all this together we have $d(S) \geq (p^2 - p - 10)(p^3 - p)/p^2(2, p - 1)^2 \geq p + 4 \geq k(S)$ for all $p \geq 5$.

3.3.2   Other groups of Lie type

The following estimate for the probability that a pair of elements generates a group of Lie type, S, was found by Liebeck and Shalev [9] answering a question of Kantor and Lubotzky [6]:

$$1 - p(S) = O(rk(S)^3 (\log_2 q)^2 q^{-rk(S)}).$$

Here, $rk(S)$ is the untwisted Lie rank of S, the rank of the corresponding simple algebraic groups over an algebraic closure of $\mathbb{F}_q$. Combining this with a result of Fulman and Guralnick [3], $k(S) \leq 27.2q^{rk(S)}$, we see that for 'large enough' S, $d(S) \geq k(S)$.

Theorem B follows by the CFSG.

4   Dihedral Groups

5 p-Groups

6   Acknowledgments

References

[1] Miklós Abért. On the probability of satisfying a word in a group. *J. Group Theory*, 9(5):685–694, 2006.

[2] R. Lyons D. Gorenstein and R. Solomon. *The classification of the finite simple groups, no.3.* American Math. Soc., Providence, Rhode Island, 1998.

[3] Jason Fulman and Robert Guralnick. Bounds on the number and sizes of conjugacy classes in finite chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.*, 364(6):3023–3070, 2012.

[4] Robert M. Guralnick and William M. Kantor. Probabilistic generation of finite simple groups. *J. Algebra*, 234(2):743–792, 2000.

[5] S. P. Norton R. A. Parker R. A. Wilson J. G. Thackray J. H. Conway, R. T. Curtis. *ATLAS of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups.* Clarendon Press, Oxford, 1985.

[6] William M. Kantor and Alexander Lubotzky. The probability of generating a finite classical group. *Geom. Dedicata*, 36(1):67–87, 1990.

[7] M. Kassabov and N. Nikolov. Words with few values in finite simple groups. *arχiv*, (1112.5484v1).

[8] Matthew Levy. Word maps with small image in simple groups. *arχiv*, (1206.1206v1).

[9] Martin W. Liebeck and Aner Shalev. The probability of generating a finite simple group. *Geom. Dedicata*, 56(1):103–113, 1995.

[10] Alexander Lubotzky. Images of word maps in finite simple groups. *arχiv*, (1211.6575v1).

[11] Attila Maróti. Bounding the number of conjugacy classes of a permutation group. *J. Group Theory*, 8(3):273–289, 2005.

[12] Attila Maróti and M. Chiara Tamburini. Bounds for the probability of generating the symmetric and alternating groups. *Arch. Math. (Basel)*, 96(2):115–121, 2011.

[13] D. Segal. *Words: notes on verbal width in groups.* Cambridge University Press, 2009.